

Anti-Spyware Software

It is estimated that nine out of 10 computers connected to the internet are infected with spyware. Simon Edwards tests eight packages designed to make sure your PC isn't one of them

If your computer starts behaving strangely, running slowly and crashing more frequently, it has probably been infected with spyware. Online criminals have realised they can use innocent-looking programs to take over your PC and steal personal information, as well as controlling it remotely for other nefarious purposes. The difference between a spyware program and a computer virus is that spyware doesn't spread itself. A PC infected with a virus tries to infect other PCs; a spyware-infested PC will not. That is not to say that spyware sits quietly on your hard disk minding its own business, though.

An infected computer may display annoying adverts, send your personal data out to websites and other systems controlled by hackers, and take part in spamming operations and other internet attacks. Over the past few years, the spyware threat has grown and here at *Shopper* we hear about more spyware infections than regular computer virus infections.

A spyware infection often happens as a result of a user running an infected program. Downloading software from untrusted, unpoliced sources such as file-sharing networks puts you at risk. Sometimes the program you download may not contain particularly harmful software, but can include a simple 'downloader' program. This connects to one or more systems on the internet and downloads the latest version of spyware that the attacker wants to install on your system.

Another common way for the bad guys to distribute spyware is to create a website, or hijack a legitimate one, and create a webpage that loads software on your PC when you view it. In some cases, you won't even know that it is happening. This is known as a 'drive-by' spyware attack.

It's clear that keeping spyware off your system is important. There are several ways to do this yourself, without relying on software. The easiest is to use your computer logged on with a Limited account. Unless you intend to install software or otherwise reconfigure your computer, there is no good reason to run as Administrator. Limited users are less likely to fall foul of automatic spyware installations. Additionally, you can force less computer-literate users of your computer to use Limited accounts. Young children and other less clued-up users are a threat to your PC's security.

Ultimately, though, you'll want some software to help protect you. It should step in when you visit a bad site and click OK when you meant Cancel. It should also detect files that contain malicious code designed to pass control of your computer to criminals.

Software developers have produced specialised software aimed at detecting and removing spyware. These are distinct from anti-virus software, which usually includes virus detection as well as the ability to block spyware. However, we do expect an anti-virus program to detect spyware, too. Anti-spyware utilities such as Spy Sweeper have recently been made available with anti-virus protection.

We've put some of the most popular and respected anti-spyware utilities to the test, including standard anti-spyware utilities, Spy Sweeper with AntiVirus 5.3, a couple of utilities designed to tidy up after an infection and our favourite anti-virus program, to compare how effective a fully featured security package is compared to a dedicated anti-spyware utility. Not all work the same way, and some are free. Read on to find out how well these different programs will protect you.

How we test Anti-spyware software

Using our dedicated ultra-secure security testing lab, we set up a web server loaded with different malicious downloads. These files, provided by security company MessageLabs, were brand new and were all present on publicly available web servers at the time of writing.

The fact that they are so new means that any security program capable of detecting them would have to be either very clever, with powerful heuristic detection, or backed up by a powerful service capable of finding the majority of spyware on the internet. If you spend good money on security software, you should expect an effective service that's capable of providing comprehensive anti-spyware updates.

We expect a good anti-spyware program to be able to prevent spyware getting on to your machine. Many of the utilities

here are capable of tracking suspicious settings, preventing certain settings from being changed and providing varying levels of spyware removal. However, our tests concentrate on the ability of these programs to prevent an infection in the first place.

Programs that provide real-time protection, and that are powered by efficient and wide-reaching anti-spyware services, should be more effective at preventing infections than free scanners such as Ad-Aware, which attempt to clean up after the event.



▲ The web server gets loaded up ready for the spyware invasion

SOFTWARE LABS

THIS MONTH

Grisoft AVG Anti-Spyware Free 7.5

Page 120

Lavasoft Ad-Aware SE Personal 1.06

Page 120

Microsoft Windows Live OneCare

Page 120

PC Tools Spyware Doctor 5

Page 121

Spybot Search & Destroy 1.4

Page 121

Steganos AntiVirus 2007

Page 121

Sunbelt Software CounterSpy 2

Page 122

Webroot Spy Sweeper with AntiVirus 5.3

Page 122



▲ AVG Anti-Spyware's scanning detection beats that of many of its competitors

GRISOFT AVG Anti-Spyware Free 7.5

★★★★★

Free

When we last tested this product, it was called ewido anti-spyware and it did pretty well defending against the relatively small number of threats we fired at it. The interface remains the same as before and the program includes a number of privacy-related tools such as options to shred files, avoid notifying Microsoft when an infection appears on the system and prevent the system appearing in other computers' My Network Places.

Initially, we had problems installing the program on our clean Windows XP test system. The program incorrectly detected that we were running a 64-bit version of Windows and refused to install. We've seen similar problems flagged on the internet, but Grisoft told us that it is rare. The company supplied us with a customised version of the software that does not attempt to detect 64-bit Windows, and this worked.

The interface is less clunky than that of AVG Anti-Virus Free, the free anti-virus program from the same company, and the underlying options are powerful, resembling those that are often found in anti-virus programs. For example, it can scan within compressed files, and this could be the reason why its scanning detection beats that of many of its competitors. That said, its real-time detection was poor and it failed to recognise any of the spyware while it was being downloaded to the hard disk.

Manually scanning the system diagnosed over 90 per cent of the files as harmful, which is a strong performance. Not only that, but manually scanning the remaining files diagnosed all but one as spyware. As non-business users can install this software for free, it is possible to combine it with AVG Anti-Virus Free to get decent all-round protection without paying a bean. If you want the best, however, you'll have to pay for Steganos AntiVirus 2007.

SUMMARY

- ✓ Lots of features
- ✓ Good detection
- ✗ Not free for businesses

ANTI-SPYWARE SOFTWARE Requires Windows 2000/XP/Vista, 300MHz processor, 64MB RAM, 70MB disk space
SUPPLIER <http://free.grisoft.com>
DETAILS <http://free.grisoft.com>



▲ Ad-Aware SE Personal is useful only after you realise your system is infected

LAVASOFT Ad-Aware SE Personal 1.06

★★★

Free

Lavasoft's Ad-Aware is a very popular free utility for removing spyware. It used to be included in Google's Google Pack, which is a free collection of essential utilities. It has now been replaced with a limited version of Spyware Doctor, possibly because the latter provides some real-time protection. The free version of Ad-Aware does not provide real-time protection. For that, you'll need to pay between £13 and £20 for either the Plus or Professional version.

Because it does not scan in real time, Ad-Aware SE Personal failed to detect any of the spyware as we downloaded it to the target system. Running a manual scan was a relatively futile exercise, too, as the program found only eight per cent of the spyware. Installing some of the spyware files did not generate any alerts, although running the scanner did find evidence of some infections.

Removing spyware using this product requires multiple reboots and an element of finger-crossing. It is impossible for regular users to know for sure if any anti-spyware or anti-virus program has fully removed an infection, so the best you can expect is for the program to list a load of problems and then delete them. After this, if the system runs faster and does not display annoying adverts, you have to assume that it is clean. That is a dangerous assumption, though.

This is a clean-up tool, useful only after you realise that your system is infected. The spyware problem has grown so fast that we don't believe you should rely on this type of protection any more. You might find this utility handy when resurrecting an infected PC, perhaps to save your files before reinstalling Windows, but it's not suitable for keeping a system up and running over a period of time. For that, you need a fully featured anti-spyware program with real-time protection.

SUMMARY

- ✓ Free
- ✗ Won't prevent an infection
- ✗ Basic features

ANTI-SPYWARE SOFTWARE Requires Windows 98/2000/XP/Vista, 160MHz processor, 24MB RAM
SUPPLIER www.lavasoft.com
DETAILS www.lavasoft.com



▲ Windows Live OneCare's interface is basic, but it detected most spyware downloaded

MICROSOFT Windows Live OneCare

★★★★★

£38 inc VAT

When we first reviewed Windows Live OneCare in *What's New: Software, Shopper* June 2007, we were disappointed by its ability to detect viruses and spyware. Compared with the fully featured anti-virus software we've seen, its results were poor. However, in this round-up of software it is one of the strongest contenders. This shows that, in some respects, an anti-virus or anti-spyware program is only as good as its last set of updates.

The program detected most of the spyware as it was downloaded, and it picked up a few more files when we ran a manual scan afterwards. There is more to Windows Live OneCare than anti-spyware and anti-virus detection, though. The firewall included in the package is superior to the one that comes with Windows as standard, and it also provides a marginally better backup program.

Windows Live OneCare's interface is quite basic, and there are few settings to play with. This is partly because it integrates closely with Windows itself. For example, it uses the Windows Updates service to download virus and spyware updates. You can also check for updates manually.

Getting hold of this program involves creating a Microsoft Windows Live ID, which you'll already have if you use Hotmail, buying a code from Microsoft, downloading the software and then activating it. You can use the software as part of a 90-day free trial first.

The price of this product seems high, but bear in mind that this includes a licence to install it on three PCs at once. At around £13 per PC, this is reasonably good value, and our tests show that the anti-spyware part of the program is more effective than Spy Sweeper, Spyware Doctor and CounterSpy, all of which cost more to run per system. We'd still rather spend a little more and get better protection from Steganos AntiVirus 2007, though.

SUMMARY

- ✓ Includes licence for three PCs
- ✓ Decent spyware protection
- ✗ Underwhelming anti-virus protection

ANTI-SPYWARE SOFTWARE Requires Windows XP, 300MHz processor, 256MB RAM
SUPPLIER <http://onecare.live.com>
DETAILS <http://onecare.live.com>



▲ Spyware Doctor has a clean interface, but its spyware detection was disappointing

PC TOOLS Spyware Doctor 5

★★

£20 inc VAT

Spyware Doctor 5's clean interface and reasonable price make it an attractive option. As with Spy Sweeper, it provides real-time protection as well as a collection of other levels of protection. For example, it monitors your web browser's settings and startup programs. It can also scan a PC for existing infections. A limited version of this program is available in Google's Google Pack collection of essential utilities.

We were more interested in how it handles incoming spyware. It did quite well in our previous anti-spyware test (*Shopper* October 2006), although its real-time protection was patchy. This time we really put it to the test, throwing many more samples of spyware on to the hard disk of the test system. The result was underwhelming; it found less than half of the threats using its real-time protection.

Manually scanning the remaining downloaded files was useless and discovered no bad files, so we resorted to running an assortment of the spyware to see what happened. Spyware Doctor did notice some of the infections, detecting the system's strange behaviour rather than recognising specific spyware files.

However, after running a small number of these programs, Spyware Doctor stopped working properly and displayed a message that read, "Swdactor.exe seems to be corrupt!" It is not surprising that purposefully running a handful of spyware will eventually swamp a system, but we'd expect an anti-spyware program to have detected more threats before it got to this stage.

This was one of the least effective tools in this group in terms of discovering spyware before it has a chance to interact with the system. Considering that you can buy Steganos AntiVirus 2007 for the same price and get significantly better protection, Spyware Doctor is poor value.

SUMMARY

- ✓ Easy to use
- ✗ Disappointing spyware detection
- ✗ Expensive

ANTI-SPYWARE SOFTWARE Requires Windows 2000/XP/Vista, 800MHz processor, 64MB RAM, 25MB disk space
SUPPLIER www.pctools.com
DETAILS www.pctools.com



▲ Spybot Search & Destroy does not provide a useful level of real-time protection

SPYBOT Spybot Search & Destroy 1.4

★★

Free

Spybot Search & Destroy is a free utility that many PC experts recommend should be part of your arsenal against spyware threats. Although it has a couple of real-time protection features, it doesn't provide the same sort of protection that the commercial products do. For this reason it is really useful only after the event of a spyware infection, rather than as a preventative measure.

An Immunize feature does let you configure Internet Explorer so that it blocks sites known to host spyware. The SDHelper system also tries to prevent Internet Explorer from downloading bad files, while the optional TeaTime feature tries to discover and block running spyware processes. Together, these attempt to monitor the system for spyware in real time.

In practice, Spybot Search & Destroy does not provide a useful level of real-time protection. It failed to detect any of our samples as we downloaded them, and neither did it recognise the spyware when we ran a manual scan. Infecting the system with some spyware and then running a scan did get some results. For the reasons we've mentioned in the Ad-Aware SE Personal review on the opposite page, this is hardly an ideal situation. We'd prefer our anti-spyware software to prevent infections rather than just trying to help afterwards.

If your goal is to create a pack of free software on a CD that you can carry around and use to help friends disinfect their PCs, then this is a useful addition. It will find and remove some threats, as will Ad-Aware. Add a copy of HijackThis! (www.merijn.org) and you're on your way to becoming an anti-spyware first-aid. But if you need to protect your own PC, ignore this kind of scanner and install an anti-spyware utility with full real-time protection.

SUMMARY

- ✓ Free
- ✗ Won't prevent an infection
- ✗ Basic features

ANTI-SPYWARE SOFTWARE Requires Windows 98 or later
SUPPLIER www.safer-networking.org
DETAILS www.safer-networking.org



▲ Steganos AntiVirus 2007 includes a number of advanced protection features

STEGANOS AntiVirus 2007

★★★★★

£20 inc VAT



Steganos AntiVirus 2007 is a rebranded anti-virus program developed by Kaspersky Lab. There is no difference between this product and Kaspersky Anti-Virus 6, apart from some different logos and the fact that this package is £8 cheaper than the original Kaspersky-branded one. It includes real-time protection for data that enters the system via email and the web, as well as providing a scanner for files on the hard disk.

This anti-virus program came out top when we last ran our extensive email and web threat tests, so we expected great things. Previously, it found just under 45 per cent of the spyware that we sent to the test system, which doesn't sound great but is as good as we've seen, beating market-leading anti-virus programs such as Norton AntiVirus, McAfee VirusScan and Trend Micro's PC-cillin.

This month, we exposed it to a brand new set of spyware and it detected 100 per cent of the files. It found each one while the test system downloaded them from our web server. This is what we hope for in an anti-spyware program. Ideally, spyware should be detected before it's saved to your hard disk, massively reducing the risk of an infection.

This fully featured anti-virus program will also detect most of the email viruses we've encountered, intercepting them as your email program receives infected messages. It also includes a number of advanced protection features that you can enable to lock down your PC and prevent certain changes being made to settings.

Easy to use, remarkably inexpensive and very effective compared with the competition, this is our choice of anti-virus and anti-spyware software. Nothing else comes close for detecting spyware, including dedicated anti-spyware programs, so buying this package means you won't have to spend any more on extra security utilities, save for a firewall.

SUMMARY

- ✓ The best spyware and virus detection
- ✓ Inexpensive
- ✗ Requires frequent updating

ANTI-SPYWARE SOFTWARE Requires Windows 98 and later, 300MHz processor, 128MB RAM, 50MB disk space
SUPPLIER www.steganos.co.uk
DETAILS www.steganos.co.uk



▲ CounterSpy 2 can scan your system to check for unsuitable security settings

SUNBELT SOFTWARE CounterSpy 2

★★★★

£13 inc VAT

CounterSpy impressed us so much when we reviewed it for the first time in *Shopper* October 2006 that we gave it a Best Buy award. This latest version has seen some cosmetic changes in the interface, but it's nice to see that the range of privacy utilities is still included, such as the History Cleaner and Secure File Eraser. It can also scan your system to check for unsuitable security settings, advising changes when it finds them.

By default, it locks certain settings, which are often the target of spyware. For example, spyware may attempt to change your web browser's default homepage, but CounterSpy monitors this and prevents unauthorised changes. Different security levels are available, from Trusting up to Paranoid. You can customise these, too.

We expected great things of this program's spyware detection. However, since the last time we tested it, we have upgraded our tests, making them tougher and more extensive. This shows in the results. CounterSpy failed to detect a single piece of spyware during the download phase of the test, although running a manual scan identified over 60 per cent of the bad files. It caught a few more pieces of spyware after we attempted to run them. This is a little disappointing, although it still puts this product ahead of rivals including Spy Sweeper and Spyware Doctor. When it detects a spyware infection it offers to create a Windows Restore Point, which is helpful.

This is one of the least expensive products available, so if you had to choose a dedicated, commercial anti-spyware program, this would be on our shortlist. It's currently available with a 50 per cent discount if you upgrade from a competing product. AVG Anti-Spyware Free was more effective, though, and has the advantage of costing nothing. Steganos AntiVirus 2007 is £7 more than CounterSpy but provides better anti-spyware protection, as well as more general anti-virus defences.

SUMMARY

- ✓ Inexpensive
- ✓ Useful general security features
- ✗ Poor real-time protection

ANTI-SPYWARE SOFTWARE Requires Windows 2000/XP/Vista, 300MHz processor, 128MB RAM, 150MB disk space
SUPPLIER www.sunbelt-software.com
DETAILS www.sunbelt-software.com



▲ Spy Sweeper with AntiVirus uses a protection system of different modules called Shields

WEBROOT Spy Sweeper with AntiVirus 5.3

SPYWARE RATING: ★★

£30 inc VAT

Spy Sweeper is one of an increasing number of anti-spyware utilities to provide real-time protection. This means that the moment some recognisable spyware is saved on the system it kicks into action and removes it, optionally saving it into a quarantine area.

The program uses a protection system that consists of different modules, known as Shields. Different parts of the program track things such as Internet Explorer's settings, important Windows files, files sent over instant messaging services and the programs that load automatically when Windows starts up.

The program can scan a PC for spyware using different options. A full scan can take a long time, but is the most effective way to clean infected PCs. The Quick Sweep option runs faster but checks fewer areas, and you can also set up a Custom Sweep, which is useful if you know what you are doing and are suspicious about certain files.

The version of Spy Sweeper we tested includes anti-virus protection by Sophos. This company makes anti-virus software for businesses; this is the first time we've seen it in a consumer product. At £30, we hoped that this program would give other anti-virus programs (most of which include anti-spyware protection as standard) a run for their money. Sadly, it allowed half of the web-based threats to download to our hard disk, though it detected and blocked the other half. Manually scanning the files that got through improved the situation slightly – it detected just over half of the spyware we downloaded.

In an effort to prove that this program could handle real-time infections, we ran a few of the downloaded files. However, the program became corrupted by one of the bad programs. Although you are unlikely to encounter such a wide and undiluted mix of spyware in one afternoon, in this test the bad guys won.

SUMMARY

- ✓ Wide range of protection settings
- ✗ Disappointing spyware detection
- ✗ Expensive

ANTI-SPYWARE SOFTWARE Requires Windows 2000/XP/Vista, 350MHz processor, 15MB RAM, 15MB disk space
SUPPLIER www.webroot.com
DETAILS www.webroot.com

Labs verdict

Anti-spyware software

A report from Webroot claims that nine out of 10 computers connected to the internet are infected with spyware. With this small range of products displaying such a wide variety of abilities, this should not be surprising.

Although the detection rates for some of these anti-spyware programs seems poor, many of these programs only kick into action while an infection is taking place, or are able to help remove an infection once it has taken hold of the PC. We do not consider this to be even close to an ideal situation, though.

Anti-spyware is like anti-virus software in many ways, and it is only as good as the service behind it. While you could improve your protection by running multiple programs, taking advantage of the combined efforts of a number of companies, this will slow down your PC considerably. Essentially, we do not think you should have to do that, and neither should you need to distinguish between a virus, Trojan and spyware. Your security software should just work, whether it is labelled anti-virus or anti-spyware.

If you are sensible, avoid the most risky places on the internet and don't share your computer with someone less careful, then you reduce the risk of a spyware infection by a lot. We recommend that you also buy Steganos AntiVirus 2007, which provides excellent anti-virus protection as well as the best anti-spyware protection we've seen. It is also a bargain at £20 including VAT.

Grisoft's Anti-Spyware Free 7.5 is the next most effective and, combined with the company's free anti-virus program, provides better protection than some commercial anti-spyware and anti-virus products. The other free utilities here will come in handy if you are ever faced with the task of reviving a thoroughly infested system. Combined with a good anti-virus program and firewall, you can probably get things up and running again.

Our results show nothing quite beats using the internet sensibly. Avoid pirated software, key generators (to unlock programs you haven't paid for), illegal copies of movies, pornography and the seedier parts of the internet, and the risk of encountering spyware falls dramatically. If you then run your PC as a Limited user and use the best utilities reviewed here, your data should remain private and your PC will stay within your control. ☑

STEGANOS AntiVirus 2007

★★★★★

